REMARKS

Claims 1-57 are pending in the present application.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 103(a)

Claims 1-57 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ekdahl et al., "SNOW – a new stream cipher", Nov. 2001 (hereinafter referred to as the Ekdahl publication) in view of U.S. Patent No. 6,560,212 B1 to Prasad et al.

The rejection of claim 1 as being unpatentable over the Ekdahl publication in view of the Prasad patent is respectfully traversed. Claim 1 recites, "A method of generating a key stream comprising: applying a cryptographic function on at least five input values selected from a first array of values to generate at least five output values; selecting at least five mask values from a second array of values; and combining the at least five output values with the <u>at least five</u> mask values to generate a key stream block for the key stream; wherein the first and second arrays are finite." In the Office Action, the Examiner recognizes that the Ekdahl publication does not teach or disclose at least five input values selected from a first array of values to generate at least five output values, selecting at least five mask values from a second array of values and combining the first at least five values with the at least five mask values to generate a key stream block. See, page 3. However, the Examiner then asserts that the Prasad patent "teaches at least five input values selected form [sic] a first array of values to generate at least five output values, selecting at least five mask values from a second array of values and combining the first at least five values with the at least five mask values to generate a key stream block (see figures 1, 2 and 5, PN sequence, Masking operation and deBRUIJN sequence etc . . .,)." See, Office Action, page 3.

Applicants respectfully disagree with the Examiner's characterization of the Prasad patent. Applicants assert that the Prasad patent teaches selecting four values, P_0, P_1, P_2, and P_3, from a delayed sequence S_Δ and combining those values with four masking values, M_{03}, M_{14}, M_{25} and M_{36}, and selecting three values, P_4, P_5 and P_6, from a sequence S and combining those values with three masking values, M_{40}, M_{51} and M_{62}, to generate an offset sequence S_O. See,

Figure 5. Applicants further assert that the Prasad patent fails to teach "applying a cryptographic function on at least five input values selected from a first array of values to generate at least five output values; selecting at least five mask values from a second array of values; and combining the at least five output values with the at least five mask values", as recited in claim 1. Instead, the Prasad patent discloses selecting four values from a delayed sequence and selecting three values from a sequence.

Further, the Examiner asserts that the Prasad patent teaches "to generate a key stream block". See, Office Action, page 3. Applicants again respectfully disagree with the Examiner's characterization of the Prasad patent. The Prasad patent teaches generating an offset sequence from a reference sequence. "An offset sequence generator generates an offset sequence from a reference sequence, the offset sequence being a cyclic shifted version of the reference sequence." See, Abstract. The Prasad patent fails to mention or discuss "a key stream block", or its generation. Instead, the Prasad patent is related to generating offset sequences for a code-division, multiple-access (CDMA) based communication scheme. Particular reference is made to generating a deBruijn sequence used in the IS-95 system. The code sequences used for communication channels in the IS-95 system are known values, and cannot be merely deemed to be a key stream block without any evidence. The Examiner has not provided any evidence that the offset sequence of the Prasad patent discloses a key stream block as recited in claim 1.

Similarly, the Ekdahl publication fails to disclose generating a key stream block. Instead, the SNOW generator of the Ekdahl publication produces a running key (Fig. 1), by bitwise adding the output of the finite state machine (FSM) with the last entry (32 bits) of the LFSR. The Ekdahl publication teaches combining only the last entry of the LFSR with the FSM output to generate the running key. Therefore, only one 32-bit entry or value of the LFSR's array of values is selected and combined in generating the running key. Generating "a key stream block" is not disclosed.

Thus, the Ekdahl publication and the Prasad patent fail to disclose or suggest all of the features recited in claim 1. Accordingly, the rejection of claim 1, as being unpatentable over the Ekdahl publication in view of the Prasad patent, should be withdrawn.

It is respectfully submitted that dependent claims 2-26 and 54 are at least allowable for the reasons given above in relation to independent claim 1. Of particular note are claims 3-5 and

7, which associate the values of the first array with a LRSR. However, in the Office Action, with respect to claim 1, the Examiner associates the FSM with the first array of values, and then, with respect to claims 3-5, the Examiner associates the LFSR with the first array. See, Office Action, pages 2-5. Thus, the rejections of claims 3-5 are inconsistent with the rejection of claim 1. Also, claim 10 recites that "the first and second arrays each comprises seventeen values". However, the FSM does not have seventeen registers, and the LFSR of the SNOW generator has only 16 registers. Further, claim 5 recites "wherein each values comprises one or more words, each of two or more bytes". In contrast, the Prasad patent suggests that the sequence values P are single bits. See, column 5, lines 52-58. Claim 54 further recites that "the key stream block comprises five or more words, each word having two or more bytes", which features are not disclosed by the Ekdahl publication and the Prasad patent, taken singly or in combination. With respect to claim 54, the Examiner notes that, in the Ekdahl publication, "each key stream block is <u>32 bits long</u>". See, Office Action, page 6. (Emphasis added). The Examiner further notes that the key size is 128 bits or 256 bits, without asserting that the key is a key stream block.

Claims 27-53 and 55-57 are apparatus and computer readable medium claims having features defined by language similar to that of method claims 1-26 and 54. Claim 27 recites "means for combining the <u>at least five</u> output values with the <u>at least five</u> mask values to generate a key stream block for the key stream", claim 37 recites, "combining the <u>at least five</u> output values with the <u>at least five</u> mask values to generate a key stream block for the key stream", and claim 44 recites, "a combining module configured to combine the <u>at least five</u> output values with <u>at least five</u> mask values selected from a second array of values to generate a key stream block for the key stream". Accordingly, for the reasons recited above with respect to claims 1-26 and 54, claims 27-53 and 55-57 define patentable advances over the Ekdahl publication and the Prasad patent, and the rejections of claims 27-53 and 55-57 should be withdrawn.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **February 17, 2009**

By:
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502